**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF DELAWARE**

| | |
|---|---|
| ICONTROL NETWORKS, INC., a Delaware corporation,<br>Plaintiff,<br>v.<br>ZONOFF INC., a Delaware corporation,<br>Defendant. | C.A. No. 14-1199-GMS |

## FINAL JOINT CLAIM CONSTRUCTION STATEMENT

Pursuant to Paragraph 2 of the Court’s April 20, 2015, Scheduling Order [D.I. 46], Plaintiff Icontrol Networks, Inc. (“Icontrol”) and Defendant Zonoff Inc. (“Zonoff”) jointly submit this Final Joint Claim Construction Statement which includes, as Exhibit 1, the disputed terms that either party contends is in need of construction,[1] the parties’ respective positions on construing

[1] Zonoff contends only the following claims are properly within the scope of this case: U.S. Pat. No. 7,262,690, claim 1; U.S. Pat. No. 6,624,750, claim 1; U.S. Pat. No. 8,612,591, claim 57; U.S. Pat. No. 8,478,871, claim 15; U.S. Pat. No. 8,638,211, claim 1; and U.S. Pat. No. 8,335,842, claims 1 and 14. Zonoff reserves its rights to propose additional terms for construction and/or additional constructions should the Court permit expansion of this case beyond the above-identified claims. Zonoff reserves, and does not waive, its right to argue that any terms are not capable of construction and/or lack sufficient support in the specification and to cite to additional intrinsic evidence in response to the claim construction briefing of Icontrol.

Icontrol disagrees with Zonoff’s contention that this case is limited to the above recited claims. On March 10, 2015, Icontrol served Zonoff with an interrogatory response identifying the following asserted claims: 1, 3, 5, 7, 13, 14, 16, and 19 of the ‘750 patent; claims 1, 2, 4, 5, and 8 of the ’690 patent; claims 1, 6-8, 10, 14, 19, 20, 21, and 23 of the ‘842 patent; claims 1, 10, 13, 16, and 20 of the ’211 patent; and claims 1, 15-18, 19, and 31 of the ’871 patent; and claims 1, 6, 7, 12, 22, 24, and 57 of the ’591 patent. On that date, Icontrol provided detailed claim charts showing Zonoff’s direct infringement of the aforementioned claims. Icontrol objects to Zonoff’s apparent refusal to identify all the terms that it believes require construction in this case.

each disputed term, and citations to intrinsic evidence for each disputed term. Exhibit 2 sets forth the parties' agreed constructions for certain claim terms.

Dated: December 21, 2015

*/s/ Mary B. Matterer*
Richard K. Herrmann, Esquire (I.D. No. 405)
Mary B. Matterer, Esquire (I.D. No. 2696)
MORRIS JAMES LLP
500 Delaware Avenue, Suite 1500
Wilmington, Delaware 19801
302.888.6800
rherrmann@morrisjames.com
mmatterer@morrisjames.com

*Attorneys for Plaintiff*
*Icontrol Networks, Inc.*

*/s/ Jody Barillare*
Colm F. Connolly, Esquire (I.D. No. 3151)
Jody Barillare (I.D. No. 5107)
MORGAN, LEWIS & BOCKIUS LLP
The Nemours Building
1007 North Orange Street, Suite 501
Wilmington, Delaware 19801
302.574.7290
cconnolly@morganlewis.com
jbarillare@morganlewis.com

*Attorney for Defendant*
*Zonoff Inc.*

# EXHIBIT 1 – DISPUTED CLAIM TERMS

| ***“control unit for receiving signals from a variety of detection devices monitoring events pertaining to security” - ’690 Patent*** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| This is not a means plus function term.<br>Plain and Ordinary meaning<br>Intrinsic Evidence: ’690 Patent, Col. 2 Li. 23-35; Col. 2 Li. 50-57; Glossary Col. 5; Figures 1 and 2 | This is a means-plus-function term.<br>Structure: ACU 50 which includes an RSC300 chip 500, a microprocessor 510, non-volatile Flash memory 501, a microphone 502 with a dual monostable 503 to control its operation and an automatic gain control 504, a speaker 520, user interface controls 506, a low power radio transmitter 507, an 868 MHz low power radio receiver, a power supply with battery backup 518, a modem 519, resistors, capacitors, and logic elements.<br>Function: receiving signals from a variety of detection devices monitoring events pertaining to security.<br>Intrinsic Evidence: ’690 Patent, Abstract (“The invention provides a monitoring and control system comprising a control unit (50) for receiving signals from a variety of detection devices (10, 21, 502) monitoring events pertaining to security.”);<br>Col. 5: Chart (“ACU: An Alarm Control Unit. This is a local control unit provided at a monitored site. The ACU is adapted to receive signals generated in response to events by detection devices also located at the monitored site, process the signals and transmit information relating to the received signals to a remote monitoring station”);<br>Col. 16 Li. 21-33 (“As illustrated in FIG. 5, the ACU (50) comprises an RSC300 chip (500), Flash (non-volatile) memory (501), a microphone (502) with a dual monostable (503) to control its operation and an automatic gain control (504), a speaker (520), user interface controls (such as buttons, lights and switches) (506), a low power radio transmitter (507), a power supply (which may be a battery, solar powered, mains supplied, or a combination thereof) and other components (resistors, capacitors, logic elements and the like) |

As illustrated in FIG. 6, the ACU (50) further comprises an 868 MHz low power radio receiver (517), microprocessor (510), some non-volatile memory, a power supply (518) with battery backup and a modem (519).");

Figure 4b:

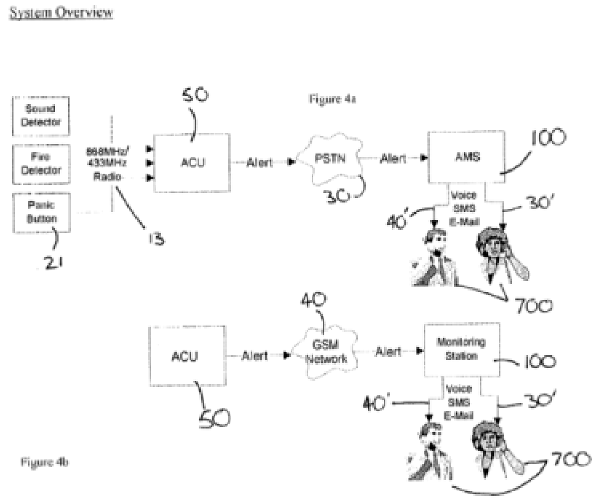


Figure 5:

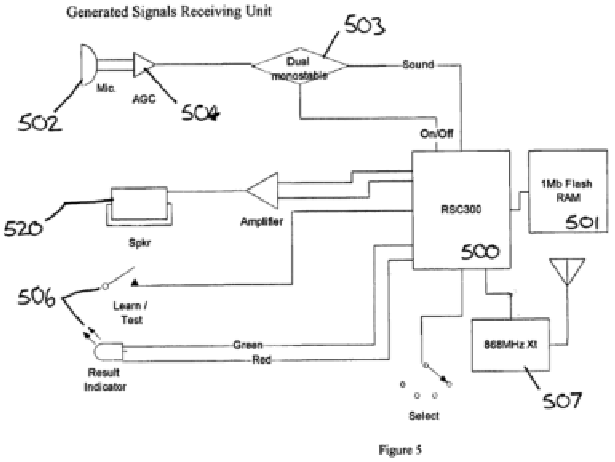
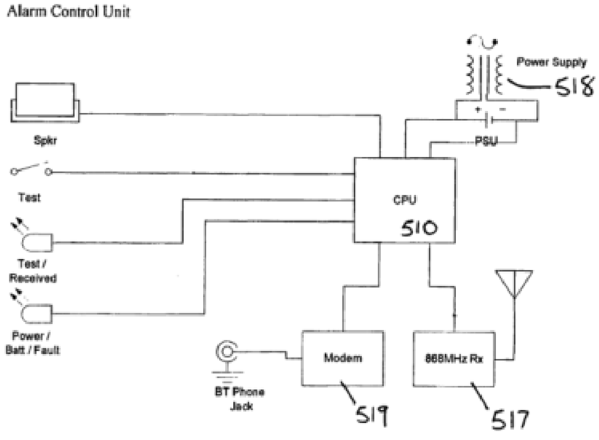
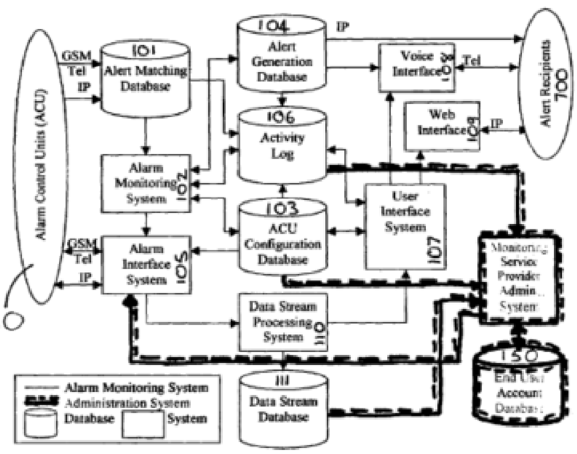


Figure 6:

| | |
|---|---|
| | <br> Alarm Control Unit<br>Power Supply<br>518<br>Spkr<br>PSU<br>Test<br>CPU<br>510<br>Test / Received<br>Power / Batt / Fault<br>BT Phone Jack<br>Modem<br>868MHz Rx<br>519<br>517<br>Figure 6<br>Col. 4 Li. 56-59 ("FIGS. 5 and 6 illustrate schematically elements of a local control unit usable in the system and constructed in accordance with the invention."). |

| ***"control means for actively controlling one or more detection devices"* - '690 Patent** | |
|---|---|
| **Icontrol's Position** | **Zonoff's Position** |
| This is a means-plus-function term<br>Structure: The structure linked to the recited function is the applicable portions of the alarm control unit (Figure 5).<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: '690 Patent, Col. 16 Li. 21-41; Figures 1, 2, 4a, 4b; 5, 6 | This is a means-plus-function term.<br>This term is not capable of construction |

| ***"means for transferring information related to the reception of such signals to a remote monitoring station"* - '690 Patent** | |
|---|---|
| **Icontrol's Position** | **Zonoff's Position** |
| This is a means-plus-function term<br>Structure: a modem<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: '690 Patent, Col. 16 Li. 21-41; Col. 17:1-5; 18:13-19; Figures 5, 6 | This is a means-plus-function term.<br>This term is not capable of construction |

<table>
<tr><th colspan="2"><em>"programmable storage means storing automatic evaluation routines to initiate the automatic transfer of information to a chosen remote user terminal"</em> - '690 Patent</th></tr>
<tr><th>Icontrol's Position</th><th>Zonoff's Position</th></tr>
<tr><td>This is a means plus function term<br><br>Structure: The structure linked to the recited function is the non-volatile memory<br><br>Function: plain and ordinary meaning<br><br>Intrinsic Evidence: '690 Patent Col. 7 Li. 27-Col. 8 Li. 23; Col. 11 Li. 31-36; Figs. 1-3</td><td>This is a means plus function term.<br><br>Structure: a combination of Alarm Monitoring System 102, Alarm Control Unit Configuration Database 103, and Alert Generation Database 104.<br><br>Function: storing routines that are configured to determine actions to be taken based upon particular types of alerts, and to instruct systems to send messages to a chosen user terminal designated to receive the messages.<br><br>Intrinsic Evidence: '690 Patent Figure 2:<br>Automatic Monitoring Station Embodiment – Logical Units<br><br>

Alarm Control Units (ACU)<br>GSM<br>Tel<br>IP<br>101<br>Alert Matching Database<br>104<br>Alert Generation Database<br>IP<br>Voice Interface<br>108<br>Tel<br>Alert Recipients<br>700<br>Web Interface<br>109<br>IP<br>106<br>Activity Log<br>Alarm Monitoring System<br>102<br>103<br>ACU Configuration Database<br>User Interface System<br>107<br>GSM<br>Tel<br>IP<br>Alarm Interface System<br>105<br>Monitoring Service Provider Admin. System<br>50<br>Data Stream Processing System<br>110<br>150<br>End User Account Database<br>111<br>Data Stream Database<br>Alarm Monitoring System<br>Administration System<br>Database<br>System

<br><br>Col. 5 Li. 6-13:<br><table><tr><td>AMS</td><td>An Automatic Monitoring Station. This has programmable storage means allowing it to identify events pertaining to security detected by detection devices and carry out actions determined by the nature of the identified event. Some of the actions will include automatically sending information pertaining to security to a chosen remote terminal. In some embodiments of the invention, a user of a monitoring system utilising the AMS may alter the actions or sequence of</td></tr></table></td></tr>
</table>

| | |
|---|---|
| | actions to be taken by instructing it from a remote terminal. |
| Alert | A signal from the ACU to the AMS indicating that a detector has been activated. The message may include the detector identity, type and information describing the nature of the alert. |
| Alert Actions | The actions that the system user has instructed the system to undertake in response to a particular type of Alert. |
| Alert Recipient | A person or device chosen to receive a message from the AMS following an Alert. |

Col. 5 Li. 55- Col. 8 Li. 59 ("With reference particular reference to FIG. 2, an AMS (100) may contain the following logical elements: …

Alarm Monitoring System (AMSys) (102)

This is the intelligence embedded within AMS (100). When an Alert is passed on from the AMD (101) the AMSys (102) consults the ACU Configuration Database (103) to decide what action to take. AMSys (102) has priority access to the ACU Configuration Database (103). Having determined the appropriate action to take the AMSys makes an entry into the Activity Log (106) and instructs other systems to carry out actions. Possible actions include: Request PIN Authentication. The Alarm Interface System (AIS) (105) phones the monitored site to request a PIN entry via a telephone handset. The recipient is given, say, three attempts or 1 minute to enter the correct PIN. If no correct PIN is entered then the Alert is treated as genuine, subject to alarm verification and the ACU (50) is instructed to sound local sirens (20) if applicable. Determine the nature of the alert. Send messages (voice, IP, SMS or Pager) to specified Alert Recipients. Make entry in Alert Action Log. Record and analyse Zoned Activation for alert verification system. Instruct Data Stream Processing System (110) to open a channel to the ACU (50) for download of sound or video, or instruct Data Stream Processing System (110) to manage transfer of sound or video from ACU for storage and possible onward transmission. Send an e-mail message

ACU Con figuration Database (ACUCD) (103)

The ACUCD (103) may contain:

System Configuration Table (SCT). A description of the current configuration of the Alarm System (identical to that stored locally in the SCT) and current alarm status, including any zones activated.

Alert Action Table. List of actions to be taken when a particular Alert is detected.

Alert Generation Database (AGD) (104)

This database oversees the transmission of messages to Alert Recipients (700) if no disarm has taken place. The AMS (100) may, in response to an Alert, identify that various Alert Recipients (700) need to be informed and the address where the alert has been activated. These recipients and the associated location and alert identifying message is passed to the AGD (104) that manages the transmission of those messages (i.e. queues, repeat attempts and so on). The AGD (104) interfaces to the Voice Interface (108) for messages using voice synthesis. For IP based messages the AGD has a direct Internet connection (30").

All Alerts, Message attempts and their result are recorded in the Activity Log (106). For example, there may be entries made containing information similar to the below, presented in a manner similar to the below:

| Date and Time | Message | Alert Recipient | Result |
|---|---|---|---|
| 15/11/00 12:19 AM | Intruder Alarm Alert Received by MyGard | N/A | N/A |
| 15/11/00 12:20 AM | Intruder Alarm Alert phone call to | (07790 926039) | No Answer |

| | | | |
|---|---|---|---|
| | Mr J. Bloggs | | |
| 15/11/00 12:20 AM | Intruder Alarm Alert pager message to Mr F. Brown | (0207 926 0394) | Sent |
| 15/11/00 12:25 AM | Retry: Intruder Alarm alert call to Mr J. Bloggs | (07790 926039) | Answered |
| 15/11/00 12.25 AM | Intruder Alarm activated at (address) Abel Security | e-mail address | Acknowledged |

The AGD will also manage communications with Police Control Rooms, private security response units and the Fire Brigade. The AGD will generally deal with jobs in First In, First Out (FIFO) order, except for Panic Alerts that receive immediate attention. Keyholders who, if police/private security are attending, will be contacted early in the alert cycle and asked to confirm their attendance automatically by pressing the * button on their phone--this action is then registered on the Action Log.");

Col. 2 Li. 35-36 ("The AMS can respond to events according to preset commands or routines, which are recorded in a database.");

Col. 12 Li. 14-54 ("Ability to Perform Actions Specified by the User in Response to an Alert
Users are able to use the User AMS interface (107) to record the actions they would like to take place when specific Alerts occur. These actions would form the basis of the pre-set routines stored on the AMS that enables the AMS to respond to events. A wide range of Alert Actions may include: Initiation of an

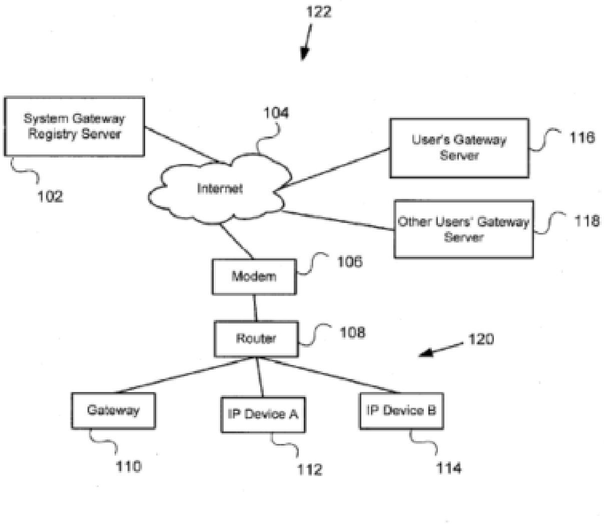
|  |  |
|---|---|
|  | Automatic False-Alarm Reduction Check Recording of the Alert in the Alert log. Automatic placement of telephone calls to Alert Recipients (700) by means of Voice Synthesis software, informing the Alert recipient of the Alert. Automatic generation of an e-mail to an Alert Recipient informing the Alert recipient of the Alert. Automatic generation of a message to a pager or other mobile device informing the Alert recipient of the Alert. Automatic recording of the Alert and subsequent Alert Actions in the Activity log (including failed attempts to carry out an Alert Action.) Specification of times of the day, days of the week and holiday periods when the Alert Action should not be carried out, for example to not call elderly relative after 10 PM to inform them of mains power failure or other minor events. Automatic notification of Alert to police, private security firm, fire brigade or other nominated party. Automatic triggering of a call to pre-determined User number, such as a mobile phone number, to ask a user whether they would like attendance by private security firm. Automatic initiation of video image capture or sound recording.<br>The Alert Recipient may be, but not essentially be, the user. The user may also nominate further Alert Recipients or nominate different recipients for Alerts relating to different events. Any number of Alert Actions can be associated with an Alert. If the AMS is unable to complete an Alert Action it should continue to attempt to complete the action for a finite period, or until the Alert is cancelled.");<br><br>Col. 1 Li. 58 – Col. 2 Li. 4 ("The invention also provides an automatic monitoring station for receiving first information related to events detectable by detection devices, the monitoring station comprising means adapted to receive such first information and programmable storage means storing:<br><br>i) routines for evaluating received first information,<br>ii) a record of actions to be taken in response to a variety of types of evaluated first information,<br>iii) routines for matching evaluated first information to a particular stored action or set of actions, and<br>iiii) routines for initiating the matched action or set of actions; wherein some actions include transferring |

| | |
|---|---|
| | second information relating to detected events to a chosen remote terminal.”);<br><br>Col. 5 Li. 59-61 (“The AMD (101) consists of a database, a telephony interface and an IP interface to receive Alerts from any ACU (50).”);<br><br>Col. 10 Li. 53-60 (“These logical units will generally be located together in one physical part of the AMS (100). FIG. 3 illustrates how the AMS can have access to the databases and application programs controlled by a firewall (120) and web buffering server (121). The firewall and web buffering server are located between the hardware storing the databases and application programs and the means for connecting to the ACU and users and Alert recipients.”);<br><br>Abstract (“The invention provides a monitoring and control system comprising a control unit (50) for receiving signals from a variety of detection devices (10, 21, 502) monitoring events pertaining to security. The control unit (50) transmits information related to the reception of such signals to a remote monitoring station (100) that stores and operates automatic evaluation routines to send an alert call to a chosen remote user terminal.”). |

| ***“proprietary to the security system”* - ’591 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| a protocol owned and/or controlled by the provider of the applicable security system component.<br><br>Intrinsic Evidence: ’591 Patent Col. 1 Li. 63-67; Col. 3 Li. 52-Col. 4 Li. 2; Col. 4 Li. 22-40; Col. 4 Li. 47-54; Col. 5 Li. 5-44; Col. 20 Li. 32-44; Col. 28:26-39; Figs. 16 and 17 | useful only with the security systems of the same vendor<br><br>Intrinsic Evidence: ’591 Patent Col. 1 Li. 63 – Col. 2 Li. 9 (“Each vendor typically has developed sophisticated proprietary wireless technologies to enable the installation and management of wireless sensors, with little or no ability for the wireless devices to operate separate from the vendor's homogeneous system. Furthermore, these traditional systems are extremely limited in their ability to interface either to a local or wide area standards-based network (such as an IP network); most installed systems support only a low-bandwidth, intermittent connection utilizing phone lines or cellular (RF) backup systems. Wireless security |

| | |
|---|---|
| | technology from providers such as GE Security, Honeywell, and DSC/Tyco are well known in the art, and are examples of this proprietary approach to security systems for home and business.”);<br><br>Col. 2 Li. 25-62 (“Due to the proprietary approach described above, the traditional vendors are the only ones capable of taking advantage of these new network functions. To date, even though the vast majority of home and business customers have broadband network access in their premises, most security systems do not offer the advanced capabilities associated with high speed, low-latency LANs and WANs. This is primarily because the proprietary vendors have not been able to deliver such technology efficiently or effectively. . . . A disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the continued proprietary approach of these vendors. As they develop technology in this area it once again operates only with the hardware from that specific vendor, ignoring the need for a heterogeneous, cross-vendor solution. Yet another disadvantage of the prior art technologies of the traditional proprietary hardware providers arises due to the lack of experience and capability of these companies in creating open internet and web based solutions, and consumer friendly interfaces.<br><br>A disadvantage of the prior art technologies of the third party hard-wired module providers arises due to the installation and operational complexities and functional limitations associated with hardwiring a new component into existing security systems. Moreover, a disadvantage of the prior art technologies of the new proprietary systems providers arises due to the need to discard all prior technologies, and implement an entirely new form of security system to access the new functionalities associated with broadband and wireless data networks. There remains, therefore, a need for systems, devices, and methods that easily interface to and control the existing proprietary security technologies utilizing a variety of wireless technologies.”); |

| | |
|---|---|
| | Col. 29 Li. 11-23 (“FIG. 17 is a block diagram of an integrated security system 1700 wirelessly interfacing to proprietary security systems, under an embodiment. A security system 1710 is coupled or connected to a Gateway 1720, and from Gateway 1720 coupled or connected to a plurality of information and content sources across a network 1730 including one or more web servers 1740, system databases 1750, and applications servers 1760. While in one embodiment network 1730 is the Internet, including the World Wide Web, those of skill in the art will appreciate that network 1730 may be any type of network, such as an intranet, an extranet, a virtual private network (VPN), a mobile network, or a non-TCP/IP based network.”). |

| ***“gateway registry”* - ’871 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| a server component that maintains records relating to the gateways.<br><br>Intrinsic evidence: ’871 Patent Col. 2, Li. 19-23; Col. 2 Li. 56-67; Col. 3 Li 6-10; Col. 3 Li 14-22; Col. 3 Li 38-39; Col. 4 Li 11-33; Col. 4 Li. 47-53; Col. 4 Li. 64-Col. 5 Li. 1; Col. 7 Li. 18-31; Col. 16 Li. 15-26; Col. 16 Li. 49-60; Col. 18 Li. 2-16; Col. 18 Li. 32-34; Col. 18 Li. 42-50; Fig. 1, 2, and 3 | a repository that associates a serial number of a specific gateway device with an address of a specific gateway server and an account<br><br>Intrinsic evidence: ’871 Patent Col. 2 Li. 21-23 (“The gateway registry communicates to the gateway the location of the server containing the account of the account associated with the gateway.”);<br><br>Figure 1:<br>  122<br>System Gateway Registry Server<br>102<br>104<br>Internet<br>User's Gateway Server<br>116<br>Other Users' Gateway Server<br>118<br>Modem<br>106<br>Router<br>108<br>120<br>Gateway<br>110<br>IP Device A<br>112<br>IP Device B<br>114<br>FIG. 1<br>Figure 2: |

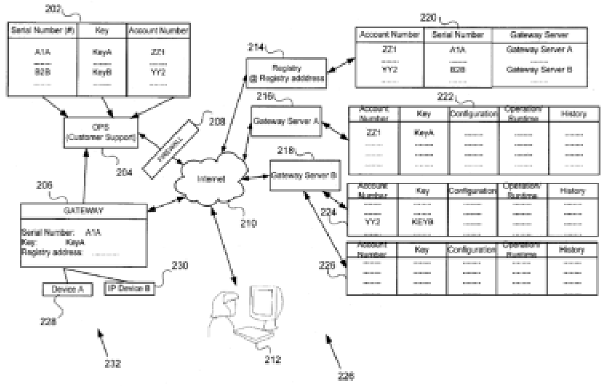


FIG. 2

Figure 3:

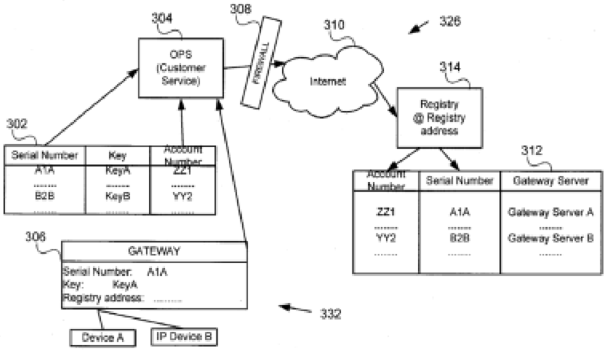


FIG. 3

Figure 4:

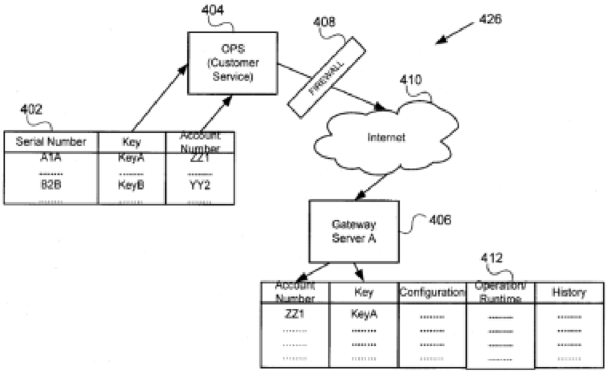


FIG. 4

Figure 5:

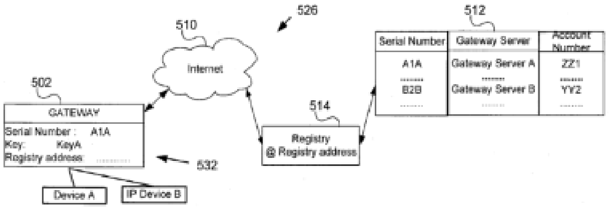


FIG. 5

Figure 8:

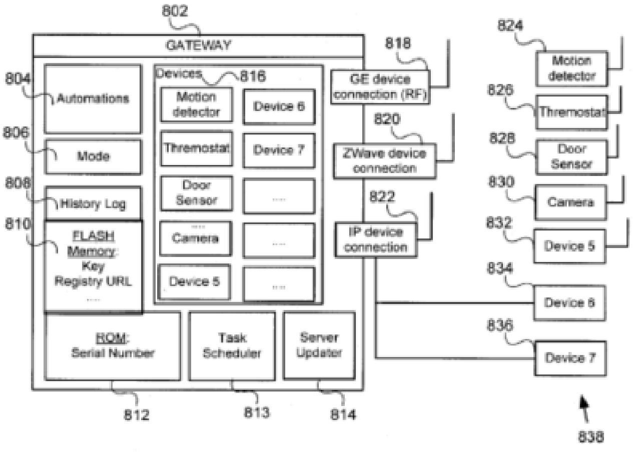


FIG. 8

Col. 2 Li 16-36 ("The gateway itself does not necessarily know what server the account is on, and thus determines, is shown, or is told which server contains the account to manage the account remotely. The methods, systems, and devices provided herein make use of a gateway registry. The gateway registry communicates to the gateway the location of the server containing the account of the account associated with the gateway. The location may comprise, for example, the address of the server. A depiction of an embodiment of a gateway registry system is provided in FIG. 1. FIG. 1 is a block diagram of a system 122 for managing control networks including a control network 120 including a gateway 110, according to an embodiment. FIG. 1 shows IP devices 112, 114 connected to router 108, a gateway 110 connected to IP devices 112, 114 through router 108 and connected through the router 108, through modem 106, and through Internet 104 to a central repository (the gateway registry 102), two gateway servers 116, 118 (user's gateway server 116 and another gateway server containing other users' accounts 118), connected through Internet 104, modem 106 and router 108 to gateway 110.");

Col. 2 Li. 56-Col. 3 Li. 22 ("For example, FIG. 2 is a block diagram of a system 226 for managing a set of control networks (for example, control network 232) With gateway devices (for example, Device A 228, IP device B 230) including a set of gateway servers

| | |
|---|---|
| | 216, 218, according to an embodiment. FIG. 2 depicts a user at a computer 212 connected to Internet 210. Further depicted is a gateway device 206 comprising the serial number (serial #) of the gateway, Which may be its MAC id or its Ethernet address, a key for the gateway, Which may be installed by the manufacturer of the gateway, and the address of the registry, Which may be a Uniform Resource Locator (URL) address for the registry server 214. In the embodiment depicted in FIG. 2, operational server (OPS) 204 is connected to database 202 (which may be called a master database or a table) which contains the serial numbers, keys and account identifications (which may be called account numbers) associated with gate ways. OPS 204 is coupled to Internet 210 through a secure connection including firewall 208. Master database 202 can be used to communicate to gateway registry 214 the serial number of the gateway 206, the account number (or account identification) associated with the gateway, and/or the server address of the account associated with the gateway. Master database 202 can be used to communicate to the gateway server account information associated with the gateway, the gateway account number, and/ or the key associated with the gateway.  Gateway registry 214 of the embodiment depicted in FIG. 2, is coupled to Internet 210, and comprises a table 220 comprising the account number and gateway servers associated with gateways serial numbers. The table 220 of the Gateway registry 214 of the embodiment depicted in FIG. 2 also comprises the addresses and/or information about which gateway servers 216, 218 connected to Internet 210 host the accounts associated with gateway account numbers and keys (which are associated with a gateway 206).”);<br>Col. 3 Li. 55 – Col. 4 Li. 6 (“Provided herein are methods and systems by which a gate way can discover the server that hosts the user’s account. Provided herein are gateway devices and/or systems which can discover the server that hosted the user’s account.<br>Each gateway device contains a unique hardware address for its Ethernet connection. Ethernet devices have unique addresses, also called gateway device |

| | |
|---|---|
| | Ethernet addresses. The Ethernet address of a gateway device may be used as a unique serial number, or another combination of numbers and letters may be used as the unique serial number for a particular gateway. In some embodiments, the gateway stores the unique hardware address for initialization of the gateway device. At production time, or thereafter, a unique key is placed in, and stored in, the gateway device. Both the unique address and the unique key are also stored in a master data base for subsequent linking to an account once the gateway is associated to an account, and/or for subsequent populating of a gateway registry table and/or subsequent populating of a gateway server table.”);<br><br>Col. 4 Li. 11-54 (“According to some embodiments, a central repository contains all known account numbers and the gateway unique numbers associated with the accounts. The location of the central repository is also stored by the gateway. In some embodiments the central repository is a gateway registry and/or gateway registry server of all known accounts and gateways. The gateway registry may also be populated with the gateway server information which may be known within the master database. Alternatively, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the registry directly, and the registry then records the server address associated with a particular account. In another embodiment, the gateway server information may be known by a third party controlling the gateway server who communicates the server information to the master database, directly or indirectly, and the master database then populates the registry with the server information associated with the account. In some embodiments, the central repository (gateway registry) is populated using a secure connection to the Internet (firewall protected) with the account number associated with the gateway device and the serial number of the gateway associated with the account number and system<br>FIG. 3 is a block diagram of a system 326 for managing control networks (for example control |

| | |
|---|---|
| | network 332) showing management of keys, serial numbers and account numbers, according to an embodiment. Shown in FIG. 3 are couplings between and information within and passed between gateway device 306, operational server master database 302, and gateway registry 314. In the embodiment of FIG. 3, the operational server (OPS) 304 and/or a customer service entity, upon association of a gateway device 306 to an account, populates a master database 302 with the account identification (which may be an account number) associated with the gateway device 306, the serial number of the gateway 306 associated with the account identification, and the key associated with the gateway 306. Operational server (OPS) 304 and/or a customer service entity, as shown in FIG. 3, may also populate a table 312 of the gateway registry 314 using a secure coupling to Internet 310 (firewall 308 protected) with the account identification associated with the gateway device 306 and the serial number of the gateway 306 associated with the account identification.”);<br><br>Col. 5 Li. 35-46 (“The central repository, in some embodiments a gateway registry and/or gateway registry server, of all known accounts and gateways is used to find which gateway server, called the account server and/or the gateway server, in some embodiments, holds the account information associated with the gateway (see, for non-limiting example, FIGS. 1 and 2). While there may be several gateway registries existing, a gateway device knows only an address for, or location of, the gateway registry which contains its gateway unique address, account identification, and the gateway server address (or location), for the gateway server holding the account associated with the gateway device.”);<br><br>Col. 5 Li. 57-Col. 6 Li. 2 (“At power-on, the gateway device initializes, and sends a request to the central repository (for example, the gateway registry) specifying only the gateway unique address, for example a serial number for the gateway or the Ethernet address for the gateway. In some embodiments, the serial number for the gateway is the Ethernet address for the gateway. This address is then used to look up the user account associated with |

| | |
|---|---|
| | the gateway unique address, and respond back to the gateway device with the location of the server that it is to use to ?nd the account associated with the gateway device. The gateway server at such location provided comprises the account associated with the gateway device which requested the information from the gateway registry.”)<br><br>Col. 6 Li. 7-12 (“The gateway server address received and the user account looked up are not sensitive, in that they are not, in and of themselves, sufficient to access the gateway server (as described herein), or to access the account on the gateway server associated with the gateway for which the unique address was provided.”)<br><br>Col. 6 Li. 13-35 (“For example, FIG. 5 is a block diagram of a system 526 for managing control networks (for example, control network 532) showing initialization of a gateway device 502, according to an embodiment. FIG. 5 is a block diagram depicting couplings between and information within a gateway device 502 and a gateway registry 514 used to execute a method of determining where the account associated with the gateway device 502 is located, and to determine the account number associated with the gateway 502. In the embodiment shown in FIG. 5, gateway 502 initializes, and sends a request to gateway registry 514 at the registry address stored in gateway memory, for example, in a table 512 of the registry 514. The request to the registry specifies the serial number for the gateway stored in the table 512. In the FIG. 5 embodiment, the serial number is used to look up the user account number associated with the gateway serial number, and the location of the server that contains the account associated with the gate way serial number. The registry 514 responds back to the gateway 502 with the account number (or account identification, in some embodiments) and location of the server that contains the account associated with the gateway. The gateway 502 stores the account number and the server location in its memory, in some embodiments.”);<br><br>Col. 7 Li 18-31(“In some embodiments, the unique |

| | |
|---|---|
| | address to user account mapping is separate from the gateway key to user account mapping. In the first mapping, the gateway device uses the gateway serial number stored Within the gateway device and the gateway registry location to contact the gateway registry in order to receive the location of the registry server and the account identification for the account associated With the gateway device. In the second mapping, the gateway device uses the location received from the registry to contact the gateway server and then uses the key stored on the gateway device and the account identification received from the registry as the bases for an authentication that unlocks the account associated With the gateway device to the gateway device.”)<br>Col. 8 Li. 45-57 (“Although not shown, the gateway device 802 of the embodiment of FIG. 8 comprises logic that, upon initialization of the gateway uses the address of the gateway registry to communicate with the gateway registry, sends a request to the gateway registry specifying the serial number of the gateway, receives a response with an address of the server upon which an account associated with the gateway is stored, and receives a response with an identification of an account for managing the location associated with the gateway; and logic that communicates with the server upon which the account associated with the gateway is stored by using the identification and authentication information derived based on the key.”);<br>Col. 9 Li. 15-Col. 10 Li. 10 (“Provided herein is a method, system, and device wherein an account may be moved from server to server as needs change (moving data-centers, etc.) without having to update the gateway devices out in the field that the server has changed. The gateway can communicate with the central repository to find the new server location by executing the method done when initializing. For example, when the gate way server containing the account associated with a particular gateway is moved, the gateway which has already executed the first mapping will not be able to access its account using the server location stored in its memory. When the gateway contacts the gateway server at the |

| | |
|---|---|
| | location it previously received from the gateway registry, it receives an error message or a non-response from the gateway server, since there is no account identification on the gateway server matching the account identification provided by the gateway device. When such error or non-response is detected by the gateway, the gateway can re-initialize (repeat the first mapping), determine the new server location and re-receive the account identification from the gateway registry, per the methods and using the devices described herein.<br>Provided herein is a method and system wherein the account associated with the gateway device (called the previous gateway device) may be associated with a new gateway device. The new gateway can be associated with an existing account on a server by first updating the master database with the new gateway serial number and new gateway key, and by associating the new key and new serial number with the account identification formerly associated with the previous gateway device. The gateway registry may then be updated by using methods and systems described herein to populate the gateway registry table with the new gateway serial number and associating the new gateway serial number with the server address associated with the previous gateway device. The gateway server may then be updated by using methods and systems described herein to populate the gateway server table with the new gateway key and associating the new gateway key with the server address associated with the previous gateway device and associating the new key with the account identification associated with the previous gateway device. Once the gateway registry and the gateway server are updated to be associated with the new gateway device, upon initialization of the new gateway (such as upon powering-on), the new gateway device can use embodiments of the methods and systems provided herein to allow remote (and/or local) management of the local management devices to which it couples. It is contemplated that a new gateway device, which is also a gateway device, may comprise the various embodiments of the gateway device as described herein.<br>An embodiment allows the gateway to not have to (although it may) store any user account information |

| | |
|---|---|
| | other than its gateway serial number, logic to communicate with the devices to which it is connected based on account information received from the gateway server, memory, a processor, inter faces to the local network of local management devices and to the local management devices that the gateway manages, interface to systems on a network remote to the location of the local management devices that the gateway manages, and logic to carry out the mappings as described herein. In some embodiments, the systems comprise the gateway registry, and the gateway server. In some embodiments, the gateway stores history of the devices on the network managed by the gateway and/or history of the gateway.”)<br><br>Col. 13 Li. 10-16 (“Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.”);<br><br>Col. 15 Li. 4-34(“In some embodiments, the gateway device comprises logic that, upon initialization of the gateway device, uses the address of the gateway registry to communicate between the gateway device and the gateway registry. In some embodiments, the logic of the gateway device sends, from the gate way device over the remote network, a request to the gateway registry specifying the serial number of the gateway device. In response to the request, in some embodiments, the logic of the gateway device receives in the gateway device, from the gateway registry over the remote network, a response including an address of a gateway server that has an account associated with the gateway device for managing the location associated with the gateway device. In some embodiments, the logic of the gateway device receives, from the gateway registry over the remote network, an identification of the account associated with the gateway device for managing the location associated with the gateway |

| | |
|---|---|
| | device. The logic of the gateway device, in some embodiments, communicates between the gateway device and the gateway server upon which the account associated with the gateway device is stored using authentication information derived based on the key, and communicates, over the remote network from the gateway device to the gateway server upon which the account associated with the gateway device is stored, the identification of the account that was received from the gateway registry and, in response to the communication of the identification of the account that was received from the gateway registry, receives account information from the gateway server.”);<br><br>Col. 16 Li. 15-27 (“The system, in some embodiments, may comprise a gate way registry including serial numbers of gateway devices of the respective control networks, identifications of accounts for the control networks, and the server address of a gateway server upon which the account associated with the control network is stored. The gateway registry may comprise logic that uses the gateway serial number of the gateway device to determine the identification of the account associated with the gateway device, logic that communicates to the gateway device the determined identification of the account associated with the gateway device and the server address of the gateway server upon which the account information is stored.”);<br><br>Col. 16 Li 49-60 (“In some embodiments, the system includes a plurality of gateway servers and wherein the gateway registry includes a set of addresses to respective gateway servers and an association between gateway device and respective gateway server. In some embodiments, the gateway registry and the gateway server are comprised by a single computer system. In some embodiments, the gateway registry includes a table having an association between each gateway serial number and corresponding account number and gateway server. In some embodiments, the gateway server includes a table having an association between each gateway account identification and corresponding key.”) |

| | |
|---|---|
| | Col. 17 Li. 7-8 ("Provided herein is a method of operating a gateway devices in a control network");<br>Col. 17 Li. 9-29 ("In some embodiments, the method of operating a gateway device in a control, network comprises storing on the gateway device an address of a gateway registry, a serial number of the gateway device, and a key. The method may further comprise using the address of the gateway registry to communicate between the gateway device and the gateway registry, and sending, from the gateway device over the remote network, a request to the gateway registry specifying the serial number of the gateway device.<br>In response to the request, in some embodiments the method comprises receiving in the gateway device, from the gateway registry over the remote network, a response including an address of a gateway server that has an account associated with the gateway device for managing a set of local management devices connected to a local network located at the location associated with the gateway device. In response to the request, in some embodiments the method comprises receiving in the gateway device, from the gateway registry over the remote network, an identification of the account associated with the gateway device for managing the location associated with the gateway device.");<br>Col. 18 Li. 2-9 ("In some embodiments, the method comprises populating a table of a gateway registry with the serial number associated with the gateway device, a gateway server location associated with an account associated with the gateway device, and the identification associated with the gateway device, wherein the serial number, the server location, and the identification are associated with each other in the gateway registry table.")<br>Col. 18 Li. 17-26 ("In some embodiments of the method for storing information to operate a gateway device in a control network, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a gateway account manager. In some embodiments of the method for storing information |

| | |
|---|---|
| | to operate a gateway device in a control network, the steps of storing the identification, populating the gateway registry table, and populating the gateway server table may be controlled by a remote management device.”);<br>Col. 18 Li. 32-34 (“The information to operate the new gateway device in the control network may be stored in a table of a gateway registry and in a table of a gateway server.”);<br>Col. 18 Li. 58 – Col. 19 Li. 19 (“The method for storing information to operate a new gate way device in a control network may further comprise populating the table of the gateway registry with the second serial number of the new gateway device by associating the second serial number with the same identification and server location previously associated with a first serial number associated with the previous gateway device, wherein a gateway server location associated with the account associated with the previous gateway device becomes the gateway server location associated with the account associated with the new gateway device, and wherein account identification associated with the account associated with the previous gateway device becomes the gateway server location associated with the account associated with the new gateway device, and wherein the second serial number of the new gateway, the server location, and the identification are associated with each other in the gateway registry table. In some embodiments, the method for storing information to operate a new gateway device in a control network may further comprise populating a table of the gateway server with a second key associated with the new gateway device by associating the second key with the identification in the table previously associated with a first key associated with the previous gateway device, wherein the account and the identification associated with the previous gateway device becomes the account and identification associated with the new gateway device, wherein the identification and the second key are associated with each other and with the account associated with the new gateway device in the table of the gateway server.”). |

| ***“means for storing configuration information for one or more security sensors”* - ’211 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| This is a means-plus-function claim.<br>Structure: the memory coupled to the processor as shown in Figure 2<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: ’211 Patent Col. 2 Li. 23-30; Col. 8 Li. 58-61; Col. 12 Li. 11-13; Col. 13 Li. 13-16; Col. 14 Li. 36-40; Col. 14 Li. 60-63; Figure 2, 6, 7, and 9 | Claim not properly in the case |

| ***“first means for communicating with the one or more security sensors”* - ’211 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| This is a means-plus-function claim.<br>Structure: a Z-Wave or Zigbee transceiver.<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: ’211 Patent Col. 4 Li. 61-64; Col. 8 Li. 42-47; Figures 1 and 2 | Claim not properly in the case |

| ***“second means for communicating with a remote server”* - ’211 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| This is a means-plus-function claim.<br>Structure: an Ethernet broadband connection or WiFi transceiver.<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: ’211 Patent Col. 4 Li. 33-36; Col. 4 Li. 54-60; Col. 5 Li. 4-8; Col. 6 Li. 23-27; Col. 6 Li. 53 – Col. 7 Li. 7; Col. 7 Li. 8-13; Col. 8 Li. 26-36; Col. 9 Li. 50-59; Col. 12 Li. 4-16; Figures 1, 2, 3, and 6 | Claim not properly in the case |

***"means for interpreting an event signal received via the first means for communicating from a first security sensor of the one or more security sensors"* - '211 Patent**

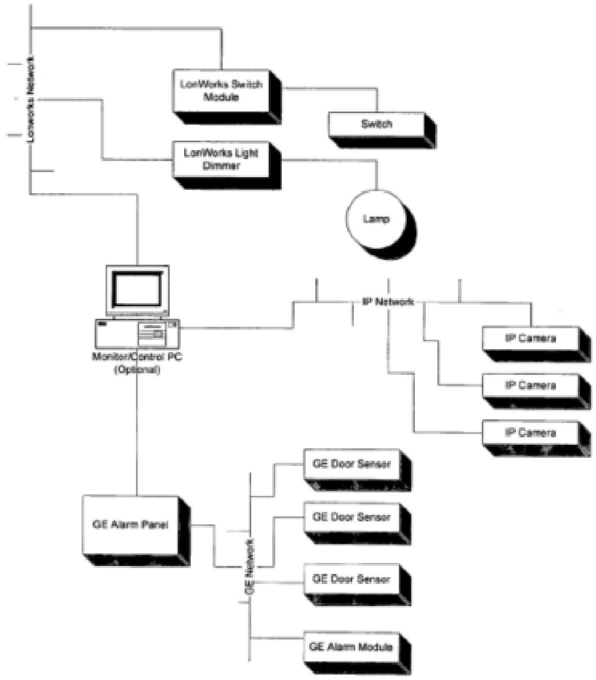
| Icontrol's Position | Zonoff's Position |
|---|---|
| This is a means-plus-function claim.<br>Structure: ARM core processor, running a micro-kernel real-time operating system with facilities for fault resilience.<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: Col. 8 Li. 13-16; Col. 9 Li. 14-42; Figures 2 and 3 | Claim not properly in the case |

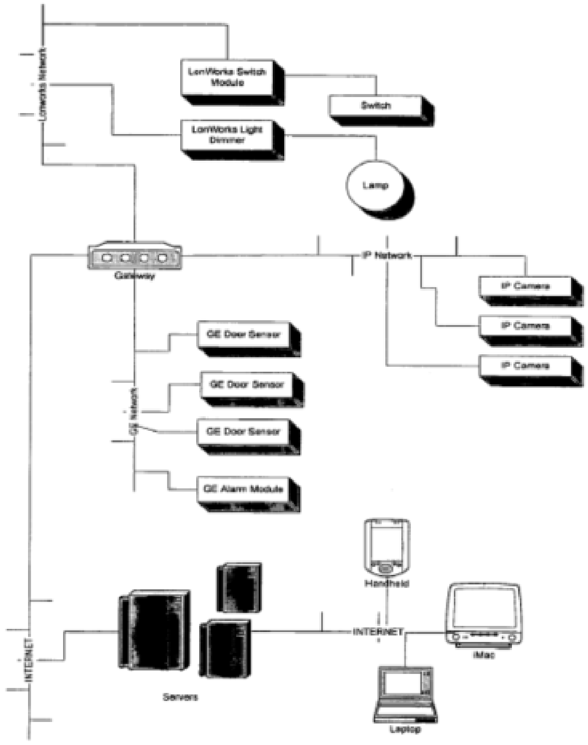
***"means for transmitting data associated with the event signal to the remote server using the second means for communicating"* - '211 Patent**

| Icontrol's Position | Zonoff's Position |
|---|---|
| This is a means-plus-function claim.<br>Structure: a service/event library and client's application program interface ("API") library components.<br>Function: plain and ordinary meaning<br>Intrinsic Evidence: '211 Patent Col. 9 Li. 43-49; Figure 2 | Claim not properly in the case |

***"autonomous network"* - '842 Patent**

| Icontrol's Position | Zonoff's Position |
|---|---|
| separate and distinct from other networks of the plurality of networks.<br>Intrinsic evidence: Col. 12 Li. 10 | a network wherein the premises management devices operate independent of other networks and devices<br>Intrinsic evidence: Figure 6: |

| | |
|---|---|
| |  Lonworks Network<br>LonWorks Switch Module<br>Switch<br>LonWorks Light Dimmer<br>Lamp<br>Monitor/Control PC (Optional)<br>IP Network<br>IP Camera<br>IP Camera<br>IP Camera<br>GE Door Sensor<br>GE Door Sensor<br>GE Alarm Panel<br>GE Network<br>GE Door Sensor<br>GE Alarm Module<br>Figure 6<br>Figure 7: |

| | |
|---|---|
| |  LonWorks Network<br>LonWorks Switch Module<br>Switch<br>LonWorks Light Dimmer<br>Lamp<br>Gateway<br>IP Network<br>IP Camera<br>IP Camera<br>IP Camera<br>GE Door Sensor<br>GE Door Sensor<br>GE Door Sensor<br>GE Network<br>GE Alarm Module<br>Handheld<br>INTERNET<br>iMac<br>Servers<br>Laptop<br>INTERNET<br>**Figure 7 - System Architecture**<br>Col. 16 Li. 21-43 ("FIG. 6 illustrates an example of a control network environment. Here three different networks with devices are depicted (GE security, LonWorks, IP). The LonWorks network includes a light switch and lamp, the GE network has some door sensors and an alarm controller, and the IP network has some IP cameras attached.<br>Note that the computer in the middle of the network may be used to bridge the various networks, essentially providing interoperability, but with available existing technologies that calls for a custom solution requiring expensive custom software. Otherwise, the three control networks are independent.<br>FIG. 7 depicts one embodiment of an architecture that uses these described concepts.<br>Here we see the same three local networks on the premises (IP, LonWorks, GE Security). However, |

| | |
|---|---|
| | now they are all connected together by the system gateway. Furthermore, the system gateway is attached to the internet, through which it regularly contacts the system servers in order to send up new data and get back control and configuration information. Clients can monitor and control their premises using ordinary browsers on a wide variety of devices by accessing the system servers.”);<br><br>’842 File History, 2011-12-12 Applicant Remarks at 11-12 (“Applicant respectfully submits that Sutton teaches autonomous devices but not autonomous networks. The Examiner cites Figure 5 as one example of Sutton's disclosure material that teaches the above referenced claim element. Sutton describes that Figure 5 illustrates how autonomous devices may be arranged in more complex configurations. Here, three networks N1, N2 and N3 are in operation. Network N1 comprises lead autonomous device 100 and two wing autonomous devices 102 and 104. Lead autonomous device 1 00 is in communication with lead autonomous device 106 from network N2. Network N2 comprises lead autonomous device 1 06 and three wing autonomous devices 108, 110 and 112. Autonomous device 112 from network N2 is in communication with autonomous device 114 from network N3. Network N3 comprises the wing autonomous device 114 and a lead autonomous device 116 (paragraph 0056).<br><br>Sutton teaches a system that coordinates communication between deployed devices. The system may establish communication channels between almost any autonomous device. Therefore, Sutton teaches autonomous devices but not autonomous networks separate and distinct from any other network (emphasis added). Sutton describes that the configuration of autonomous devices resembles that of a biological system or neural network. Note that any of the constituent networks may itself comprise other smaller-scale networks of autonomous devices (paragraph 0057). Under the teaching of Sutton, a group of constituent networks coordinate activity of autonomous devices. Accordingly, Sutton teaches autonomous devices but not autonomous networks separate and distinct from any other |

| | |
|---|---|
| | network (emphasis added).<br>Sutton further teaches that in addition to different configurations of networks of autonomous devices, a network of networks can also be dynamically reconfigured. Devices which are members of one subsystem or smaller scale network may be diverted to operate as members of another subsystem or network according to the greater need of the system at any given time (emphasis added, paragraph 0098). The system of Sutton manages resources of all sub-networks and can reconfigure device assignments at any time. Clearly, Sutton teaches directly away from an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added), and Sutton does not teach monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added). Additionally, Sutton does not describe the gateway selectively forming and controlling an associative binding between the plurality of networks (emphasis added).") (all emphasis in original);<br>'842 File History, 2011-12-12 Applicant Remarks at 13 ("Therefore, Bhat describes an evacuation system that includes detectors coupled to each of a number of fire alarm control panels, and each fire alarm control panel is coupled to a gateway (emphasis added). However, in contrast to claim 1, Bhat does not describe monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added).") (all emphasis in original); |

| | |
|---|---|
| | ’842 File History, 2011-12-12 Applicant Remarks at 14 (“Therefore, Bendinelli describes two separate gateways each of which is coupled to a separate local network, where the two gateways are also coupled to a control system via a communication channel (emphasis added). However, in contrast to claim 1, Bendinelli does not describe monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added).”) (all emphasis in original). |

| ***“the gateway selectively forming”* - ’842 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| the gateway selectively creates an associative binding<br><br>Intrinsic evidence: ’842 Patent Col. 19 Li. 1-10; Col. 20 Li. 21-36; Fig. 10, 11 | the gateway establishing without user intervention<br><br>Intrinsic evidence: ’842 Patent Col. 6 Li. 5-22 (“Homeowner configures Home (Alarms, Notifications, Binding, etc.)<br><br>This is the normal use of the system manager portal whereby the user selects the various monitoring, logging and notification options.<br><br>Future Devices are Added to System<br><br>The end user obtains additional devices from the system manager, in which case they are added to the end user system by the system manager before being shipped to the customer.<br><br>Alternatively, the end user could purchase a device from a third party source in which case they could use the system manager portal interface to add (or replace) the device manually.<br><br>In addition, the system manager gateway can have a provision for “discovering” devices by listening for RF messages (e.g., GE Interlogix) or service pin messages (e.g., LonWorks devices).”); |

| | |
|---|---|
| | Col. 19 Li. 17-27 (“User Data Abstraction<br>In an embodiment of the system, the user knows the semantics of the data, but may not know the raw data formats. So the user knows that “when I press the lamp on button on my remote, I want the lamp to go to full brightness.” Because the data from both the sensor and the actuator involved in a binding is normalized to standard data units, the user can specify their desired bindings using those standard data formats, and the system receives these selections. (In the above case, Remote “lamp” button=“On” causes the Lamp to be set to “100%”).”)<br><br>’842 File History, 2011-03-14 Claim amendments at 2-3: (“**IN THE CLAIMS**<br>What is claimed is:<br>1. (Currently amended) A method for premises management networking of a premises management system, the method comprising:<br>monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices from a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks;<br>controlling the premises management devices ~~connected to the gateway at the premises~~, the controlling comprising the gateway selectively forming and controlling an associative binding between the plurality of networks;<br>obtaining an assigned server address, and using the assigned server address for all subsequent uplink connections unless the assigned server address is changed later by the system;<br>initiating, by the gateway, all communications with a network operations center server ~~or remote user, and said all communications are initiated only based on:~~<br>~~(1) communication initiated by the gateway based on a predetermined schedule,~~<br>~~or~~<br>~~(2) communication initiated by the gateway based on an event, or~~ |

| | |
|---|---|
| | ~~(3) communication initiated by the gateway in response to an alarm condition determined from the premises management devices, or~~<br>~~(4) communication initiated by the gateway in response to receiving, at the premises, an uplink initiation signal associated with the network operations center server;~~<br>~~wherein, all communications between the gateway and the network operations center server are initiated from the gateway at the premises,~~ using the assigned server address; and<br>communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices, wherein the assigned server address is an address associated with the network operations center server.”);<br><br>’842 File History, 2011-03-14 Applicant remarks at 10-11 (“Naidoo describes that the security gateway may include a user interface that can activate or deactivate security system. In the illustrative embodiment of Naidoo, user interface is operatively coupled to keypad (paragraph 0089). The user interface of Naidoo may further include a display for displaying information to the user, where such information may include, without limitation, the current system status, whether an alarm condition has been detected, whether any components have failed, and other non-system related information such as the time, date, weather forecasts, and news bulletins (paragraph 0090).<br><br>Therefore, Applicant submits that Naidoo describes a security system having one or more sensors coupled to a security gateway, and one or more video cameras that are operable to capture video data of monitored premises, where the security gateway may be configured to create an association between one or more sensors and an associated video camera (emphasis added). However, in contrast to amended claim 1, Naidoo does not describe monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices form a plurality of networks, wherein each network of the plurality of networks |

| | |
|---|---|
| | comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added). Additionally, Naidoo does not describe the gateway selectively forming and controlling an associative binding between the plurality of networks.”);<br><br>’842 File History, 2011-12-12 Applicant Remarks at 8 (“Naidoo describes that the security system includes one or more sensors coupled to security gateway for the purpose of detecting alarm conditions (paragraph 0033). The security system also includes one or more video cameras that are operable to capture video data of monitored premises (paragraph 0034). Naidoo describes that the security gateway may be configured to create an association between one or more sensors and an associated video camera (paragraph 0034).”);<br><br>’842 File History, 2011-12-12 Applicant Remarks at 9-10 (“Naidoo describes that the security gateway may include a user interface that can activate or deactivate security system. In the illustrative embodiment ofNaidoo, user interface is operatively coupled to keypad (paragraph 0089). The user interface of Naidoo may further include a display for displaying information to the user, where such information may include, without limitation, the current system status, whether an alarm condition has been detected, whether any components have failed, and other non-systemrelated information such as the time, date, weather forecasts, and news bulletins (paragraph 0090).<br><br>Therefore, Applicant submits that Naidoo describes a security system having one or more sensors coupled to a security gateway, and one or more video cameras that are operable to capture video data of monitored premises, where the security gateway may be configured to create an association between one or more sensors and an associated video camera (emphasis added). However, in contrast to claim 1, Naidoo does not describe monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices |

| | |
|---|---|
| | form a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks (emphasis added). Additionally, Naidoo does not describe the gateway selectively forming and controlling an associative binding between the plurality of networks (emphasis added).”). |

| ***“associative binding”* - ’842 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| coupling the output of one device (a sensor) to another device (an actuator).<br><br>Intrinsic Evidence: ’842 Patent Col. 18 Li. 30-33; Figure 9 | a connection mechanism on the gateway that maps source device properties+values to destination device properties+values without containing code to do data conversion from the source device's data format to the destination device's data format<br><br>Intrinsic Evidence: ’842 Patent Col. 18 Li. 40-45 (“Gateway binding can be implemented without associative binding. That may, however, involve the gateway containing code to do the data conversion from the source device properties+values where each entry may include index of the source device property, index of the target device property, source property value anddevice's data format to the destination property value.”device's data format. For example, if a switch is bound to a lamp controller, switching the switch to on causes the lamp to turn on.” );<br><br>Col. 18 Li. 46-63 (“Associative Binding<br><br>The gateway implements a form of associative binding, where a binding (connection) is triggered by the value of a source device property. Bindings are kept in a table that maps source device properties+values to destination device properties+values. For example, consider a remote control that sends out a numeric value (for example, 1 to 10). Binding entries can map the individual values to different target devices, so that each value can turn on a different lamp. Furthermore, the binding entries contain the specific values that need to be sent to the target device property.<br>Each associative binding defined on the gateway may include: |

| | |
|---|---|
| | Index of the source device property<br>Index of the target device property<br>Source property value<br>Destination property value”);<br><br>App No. 60/652,475 2005-02-11 Preliminary Disclosure, Specification at 7-8: (“ **2.4 Associative Binding**<br>Binding is the process of “connecting” the output of one device (a sensor) to another device (actuator). An example is a switch that triggers a light to go on.<br><br>**2.4.1 Gateway Binding**<br>First, whether the devices in question use the same technology or not, associative binding uses the gateway itself as the “connection” mechanism. The gateway receives the signals from the sensor, interprets them, and relays the appropriate message to the actuator.<br><br>Gateway binding can be implemented without associative binding. But that may involve the gateway containing code to do the data conversion from the source device’s data format to the destination device’s data format. For example, if a switch is bound to a lamp controller, switching the switch to on causes the lamp to turn on.<br><br>**2.4.2 Associative Binding**<br>The gateway implements a form of associative binding, where a binding (connection) is triggered by the value of a source device property. Bindings are kept in a table that maps source device properties+values to destination device properties+values. For example, consider a remote control that sends out a numeric value (say 1 to 10). Binding entries can map the individual values to different target devices, so that each value can turn on a different lamp. Furthermore, the binding entries contain the specific values that need to be sent to the target device property.”). |

| ***“an assigned server address”* - ’842 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| an address assigned by a server. | address of the server that is assigned to the gateway prior to the first uplink connection |

| | |
|---|---|
| Intrinsic Evidence: ’842 Patent Col. 10 Li. 64 - Col. 11 Li. 3; Col. 21 Li. 29-37 | Intrinsic Evidence: ’842 Patent Col. 5 Li. 45-61 (“Gateway is Registered<br>This step involves the association of the user account on the system manager server (established in the previous step) with an actual gateway in the user's home. The gateway is connected to a broadband network or the telephone line in the home.<br><br>For this step, the installer, for example, presses a SYNCH button on the gateway, and initiates an uplink communication from the gateway to the system manager server using a default (first-time) IP address or, in the case of a dial-up-only connection, a toll free number dial by the gateway.<br><br>Upon establishing a connection with the server and locating its corresponding user account (e.g., established in a prior step), the gateway acquires a system manager server IP address (to be used from that point on for all gateway to server communication), and changes its state from unregistered to registered.”);<br><br>Col. 10 Li. 59 – Col. 11 Li. 3(“Communication with Server<br><br>The gateway can initiate all communications with the server. Gateway communication can either initiate based on a predetermined schedule (e.g., every 30 minutes) or due to a local premises alarm (selected by the user).<br><br>Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.”);<br><br>’842 File History, 2009-03-09 Applicant Remarks at 7 (“The cited disclosure of Naidoo discusses that the IP address of a security gateway may be assigned via DHCP. The cited disclosure of Naidoo fails to |

| | |
|---|---|
| | disclose obtaining an assigned server address, let alone obtaining the assigned server address wherein communications between the gateway and the network operations center server are initiated from the gateway, using the assigned server address.”);<br>’842 File History, 2009-07-31 Applicant Remarks at 7 (“Moreover, the cited disclosure of Naidoo discusses that the IP address of a security gateway may be assigned via DHCP (Naidoo page 9, par. 0083). The cited disclosure ofNaidoo fails to disclose obtaining an assigned network operations center server address, let alone obtaining the assigned network operations center server address wherein communications between the gateway and the network operations center server are initiated from the gateway, using the assigned network operations center server address. In fact, the cited disclosure of Naidoo focuses on using a gateway address, rather than a server address, by disclosing a media handler that may be responsible for keeping track of the network addresses for all security gateways (Naidoo page 10, par. 0097).”);<br>’842 File History, 2009-09-15 Applicant Remarks at 8 (“Moreover, the cited disclosure of Naidoo discusses that the IP address of a security gateway may be assigned via DHCP (Naidoo page 9, par. 0083). The cited disclosure of Naidoo fails to disclose obtaining an assigned server address associated with the network operations center (which is not a gateway address), let alone obtaining the assigned network operations center server address wherein communications between the gateway and the network operations center server arc initiated from the gateway, using the assigned server address. In fact, the cited disclosure of Naidoo focuses on using a gateway address, rather than a server address associated with the network operations center, by disclosing a media handler that may be responsible for keeping track of the network addresses for all security gateways (Naidoo page 10, par. 0097).”);<br>’842 File History 2009-11-11 Applicant Remarks at 8 (“Moreover, the cited disclosure of Naidoo discusses that the IP address of a security gateway may be |

| | |
|---|---|
| | assigned via DHCP (Naidoo page 9, par. 0083). The cited disclosure of Naidoo fails to disclose obtaining an assigned server address associated with the network operations center (which is not a gateway address), let alone obtaining the assigned network operations center server address wherein communications between the gateway and the network operations center server arc initiated from the gateway, using the assigned server address. In fact, the cited disclosure of Naidoo focuses on using a gateway address, rather than a server address associated with the network operations center, by disclosing a media handler that may be responsible for keeping track of the network addresses for all security gateways (Naidoo page 10, par. 0097).”);<br>’842 File History 2010-06-30 Applicant Remarks at 10 (“Moreover, the cited disclosure of Bendinelli fails to hint at or suggest obtaining an assigned network operations center server address wherein all communications between the gateway and the network operations center server are initiated from the gateway, using the assigned server address. As previously noted, Bendinelli does not hint at or suggest that all communications between the gateway and the network operations center are initiated from the gateway, let alone that they are initiated from the gateway using the assigned network operations center server address. By contrast, Bendinelli describes a scenario where a network operations center server establishes a tunnel with a gateway. Bendinelli provides a scenario where the network operations center determines the virtual IP address for each of the consenting gateways, and adds the consenting gateways to a partner list, and forwards the partner list to each of the consenting gateways (Bendinelli, page 19, par. 0224).”). |

| ***“initiating, by the gateway, all communications with a network operations center server using the assigned server address”* - ’842 Patent** | |
|---|---|
| **Icontrol’s Position** | **Zonoff’s Position** |
| when the gateway initiates communications with a network operations center, the gateway does so using the assigned server address<br>Intrinsic Evidence: ’842 Patent Col. 10 Li. 29-31 | all communications between the gateway and the network operations center server are initiated by the gateway and use the assigned server address<br>Intrinsic Evidence: ’842 Patent Col. 10 Li. 59-Col. 11 |

| | |
|---|---|
| | Li. 3(“Communication with Server<br><br>The gateway can initiate all communications with the server. Gateway communication can either initiate based on a predetermined schedule (e.g., every 30 minutes) or due to a local premises alarm (selected by the user).<br><br>Gateways can contact a common server for their first uplink connection in order to obtain their assigned gateway server address, which they can use for all subsequent uplink connections (unless changed later by the system). In the event that the gateway cannot connect to its designated gateway server, it can fall back to contacting the default initial gateway in order to refresh its gateway server address.”);<br><br>Col. 11 Li. 39-43 (“Implementing shoulder tap over IP is another embodiment with a more complicated installation process (e.g., router/firewall configuration, opening ports, etc.). Keeping an IP connection alive between the gateway and server can be unreliable and could heavily burden the server.”);<br><br>’842 File History, 2008-08-27 Applicant Remarks at 8 (“All communications between the server (network operations center server) and the gateway are initiated by the gateway. In contrast, Alexander does not disclose a system or method where communications are initiated by the gateway (the premises server in Alexander, see [0009]).”);<br><br>‘842 File History, 2008-09-03 Examiner Interview Summary (“Applicant’s representative provided clarification of claim 1, regarding the gateway device performing all of the initiating of all communication.”);<br><br>’842 File History, 2009-03-09 Applicant Remarks at 7 (“The distributed monitoring and video security system disclosed in Naidoo is distinct from the claimed method for premises management networking. Naidoo pertains to a distributed monitoring environment configured such that a remote user may be authenticated by a security system server, and the security system server may |

| | |
|---|---|
| | create a data connection between the remote user and a security gateway which may bypass the security system server (page 4, para. 0040, 0041 ). The user may have an account that provides full access to their respective associated security gateway (page 11, para. 01 04). The remote client may connect directly to the security gateway and provide an initial communication in the form of an access token (page 12, para. 0114).<br><br>Hence, Naidoo does not disclose a method for premises management networking comprising "initiating, by the gateway, all communications with a network operations center server or remote user, and said communications are only based on: (1) communication initiated by the gateway based on a predetermined schedule, or (2) communication initiated by the gateway based on an event, or (3) communication initiated by the gateway in response to an alarm condition determined from the premises management devices, or ( 4) communication initiated by the gateway in response to receiving, at the premises, an uplink-initiation signal associated with the network operations center server," as required by independent claim 1 (emphasis added). By contrast, Naidoo teaches that an application server may be configured to allow a remote client to initiate a two-way streaming audio connection with a security gateway (page 12, para. 0106).”);<br><br>’842 File History, 2009-07-31 Applicant Remarks at 7 (“Claim 1 of the instant application is drawn to a method for premises management networking. The claim requires initiating, by the gateway, communications with a network operations center server or remote user. That is, communications between the network operations center server or remote user and the gateway are initiated by the gateway. Furthermore, the claim requires obtaining an assigned network operations center server address, wherein communications between the gateway and the network operations center server are initiated from the gateway at the premises, using the assigned network operations center server address. These limitations are not taught by the combination of Naidoo and Bhat.”); |

| | |
|---|---|
| | ’842 File History, 2009-09-15 Applicant Remarks at 7 (“Claim 1 of the instant application is drawn to a method for premises management networking. The claim requires initiating, by the gateway, communications with a network operations center server or remote user. That is, communications between the network operations center server or remote user and the gateway are initiated by the gateway. Furthermore, the claim requires obtaining an assigned server address, wherein the assigned server address is an address associated with the network operations center server, and wherein communications between the gateway and the network operations center server are initiated from the gateway at the premises, using the assigned server address.”);<br>’842 File History, 2009-11-11 Applicant Remarks at 7 (“The claim requires initiating, by the gateway. communications with a network operations center server or remote user. That is, communications between the network operations center server or remote user and the gateway are initiated by the gateway.”);<br>’842 File History, 2010-06-30 Applicant Remarks at 7 (“The claim requires initiating, by the gateway. communications with a network operations center server or remote user. That is, communications between the network operations center server or remote user and the gateway are initiated by the gateway.”);<br>’842 File History, 2010-09-14 Non-Final Rejection at 10-12 (“For independent claims 1, 9 and 17, applicant argues that the combination of Naidoo-Bhat-Bendinelli does not teach the limitation of initiating, by the gateway, communications with a network operations center server or remote user, furthermore obtaining an assigned server address, wherein the assigned server is an address associated with the network operations center server, and wherein communications between the gateway and the network operations center server are initiated from the gateway at the premises, using the assigned |

server address. And applicant explicitly states in the arguments that the uplink-initiation signal is not a communication.

The combination of Naidoo-Bhat-Bendinelli as a whole does indeed teach the above limitations. The examiner is confused to see on how uplink-initiation signal is not communication, when the specification of the applicant's invention clearly disclose on how uplink-initiation is a communication.

The following sections display the use of uplink-initiation signal from the specs in paragraphs [0036], [0080], [0085], [0124], [0188] [0036] FIG. 5 shows a diagram of a method for premises management networking. In 510, premises management devices connected to a gateway at a premises are monitored. In 520, premises management devices connected to the gateway at the premises are controlled. In 530, an uplink-initiation signal associated with a network operations center server is received at the premises. In 540, in response to the uplink-initiation signal, communications between the gateway and the network operations center server are initiated from the gateway at the premises. In 550, during the communications between the gateway and the network operations center server, information associated with the premises management devices is communicated.

[0080] For this step, the installer, for example, presses a SYNCH button on the gateway, and initiates an uplink communication from the gateway to the system manager server using a default (first-time) IP address or, in the case of a dial-uponly connection, a toll free number dial by the gateway.

[0085] This is done on a regular basis and can always be initiated by the gateway. The server dictates the interval for uplink communication initiation between the gateway and server.

[0124] The user can specify alarm conditions for variables with discrete states (e.g., binary ON/OFF). These alarms can be reported in real-time (i.e .. immediate uplink) by the gateway to the server. The

| | |
|---|---|
| | server then in turn looks at the data and determines, based on user alarm settings, whether to notify the user or not.<br><br>[0188] The system can send variable control information downlink based on variable information collected through the uplink connection. This rule-based exchange can take place within the same atomic uplink-downlink (request-response) exchange between the gateway and server. The user specifies the actual "rules" for such bindings (e.g., turn off the thermostat when there is no motion in the premises for 2 hours).<br><br>It is clearly seen from the applicant's own invention that the use of uplink-signal is communication, because it involves communication between the network operations center server and the gateway at the client's premises. The examiner would appreciate if the applicant could clarify on how uplink-initiation signal is not communication, as it is clearly seen that the uplink-initiation signal is directed towards the network operation center server from the premise gateway.”);<br><br>’842 File History, 2011-03-14 Claim Amendments at 2-3 (“**IN THE CLAIMS**<br>What is claimed is:<br>1. (Currently amended) A method for premises management networking of a premises management system, the method comprising:<br>monitoring premises management devices connected to a gateway at a premises, wherein the premises management devices from a plurality of networks, wherein each network of the plurality of networks comprises a plurality of premises management devices forming an autonomous network that is separate and distinct from any other network of the plurality of networks;<br>controlling the premises management devices ~~connected to the gateway at the premises~~, the controlling comprising the gateway selectively forming and controlling an associative binding between the plurality of networks;<br>obtaining an assigned server address, and using the assigned server address for all subsequent |

| | |
|---|---|
| | uplink connections unless the assigned server address is changed later by the system;<br>initiating, by the gateway, all communications with a network operations center server ~~or remote user, and said all communications are initiated only based on:~~<br>~~(1) communication initiated by the gateway based on a predetermined schedule,~~<br>~~or~~<br>~~(2) communication initiated by the gateway based on an event, or~~<br>~~(3) communication initiated by the gateway in response to an alarm condition determined from the premises management devices, or~~<br>~~(4) communication initiated by the gateway in response to receiving, at the premises, an uplink initiation signal associated with the network operations center server;~~<br>~~wherein, all communications between the gateway and the network operations center server are initiated from the gateway at the premises,~~ using the assigned server address; and<br>communicating, during the communications between the gateway and the network operations center server, information associated with the premises management devices, wherein the assigned server address is an address associated with the network operations center server.”). |

## EXHIBIT 2 – CLAIM TERMS WITH AGREED CONSTRUCTIONS

| *“monitoring station”* - ’690 Patent |
|---|
| remote monitoring station located remote of the control unit |

| *“zone”* - ’211 Patent |
|---|
| grouping based on location of one or more security sensors within the premises |

| *“uplink connections”* - ’842 Patent |
|---|
| a communications link from a gateway to a server |